## AMENDMENTS TO THE SPECIFICATION:

***Please amend the paragraphs beginning at page 10, lines 11-20, as follows:***

This arrangement is illustrated in FIG. 5 of the accompanying drawings. In FIG. 5, a legacy host 12 is shown communicating with a HIP-enabled node 14 (having the domain name "hip.foo.com") via a HIP proxy node 16. The legacy host 12 accesses the HIP proxy node 16 over an access network 18 while the HIP proxy node 16 accesses the HP node 14 over the Internet 20. To partially secure the connection between the legacy host 12 and the HIP node 14, all communications between the HIP proxy node 16 and the HIP node 14 are through a Security Association set up between the HIP proxy node 16 and the HIP node 14 in a similar way to that described above with reference to FIG. 3.

However, even before the Security Association 22 shown in FIG. 5 can be set up to enable communication between the legacy host 12 and the HIP node 14, a problem arises when the legacy host 12 tries to resolve the IP address of the HIP node 14 by sending a query to a DNS server 24-1 (and in turn DNS server 24-2) when the HIP node 14 is located behind a Forwarding Agent 26 as described above. The DNS server 24-1 will return the HIT of the HIP node 14 together with the IP address of the Forwarding Agent 26. As the legacy host 12 is not HIP enabled, it will disregard the HIT and start sending messages to the Forwarding Agent 26. Without the HIT, the Forwarding Agent 26 will not be able to resolve the destination address of these messages since it is most likely that several HIP nodes will use the same Forwarding Agent 26. Likewise, since the legacy host 12 discards the HIT and uses only the IP address of the HIP node 14 when initiating a connection, the HIP proxy node 16 is unable to initiate HIP negotiation between itself and the HIP node 14 because it does not know the HIT of the HIP node 14.

***Please amend the paragraphs beginning at page 11, lines 7-29, as follows:***

According to a first aspect of the present invention there is provided a method of at least partially securing communications, via a HIP proxy node, between a first host which is not HIP enabled and a second host which is HIP enabled, the method comprising: sending a query from the first host to resolve the IP address of the second host; in response to said query, retrieving an. IP address and HIT associated with the second host, returning from the HIP proxy node a substitute IP address associated with the second host, and maintaining at the HIP proxy node a mapping between the substitute IP address, the retrieved IP address and the retrieved HIT; and upon receipt of a session initiation message at the HIP proxy node from the first host including as its destination address the substitute IP address, using the mapping to negotiate a secure HIP connection between the ~~proxy~~ HIP proxy node and the second host.

The method may comprise looking up the retrieved IP address and the retrieved HIT from the mapping based on the substitute IP address in the session initiation message, and performing the HIP negotiation using the retrieved IP address and the retrieved HIT to locate and identify the Responder together with an IP address and HIT of the ~~proxy~~ HIP proxy node to locate and identify the Initiator.

The retrieved IP address may be the IP address of a Forwarding Agent used by the second host, and further comprising initiating the HIP negotiation between the ~~proxy~~ HIP proxy node and the second host by sending the initial HIP negotiation packet to the Forwarding Agent.

The method may further comprise, following receipt of the actual IP address of the second host at the ~~proxy~~ HIP proxy node during the HIP negotiation, including the actual IP address in the mapping maintained at the ~~proxy~~ HIP proxy node. The retrieved IP address may be replaced in the mapping by the actual IP address following its receipt at the ~~proxy~~ HIP proxy node.

***Please amend the paragraphs beginning at page 12, lines 3-13, as follows:***

The method may further comprise, for an outgoing message received at the ~~proxy~~ HIP proxy node after the secure HIP connection has been established including as its destination address the substitute IP address, using the mapping to route the message over the secure HIP connection to the second host. This may entail looking up the actual IP address and the retrieved HIT from the mapping based on the substitute IP address in the outgoing message, and routing the outgoing message to the second host using the actual IP address and the retrieved HIT to locate and identify the destination of the message, and using an IP address and HIT of the ~~proxy~~ HIP proxy node to locate and identify the source of the message.

The method may further comprise completing the establishment of communications between the first and second hosts by forwarding the session initiation message from the ~~proxy~~ HIP proxy node to the second host over the secure HIP connection, replying with a session acknowledgment message from the second host to the ~~proxy~~ HIP proxy node over the secure HIP connection, and routing the session acknowledgment message to the first host. The session acknowledgment message may be a TCP ACK message.

***Please amend the paragraphs beginning at page 12, line 21 through page 14, line 6, as follows:***

The method may further comprise, for an incoming message received at the ~~proxy~~ HIP proxy node from the second host over the established secure HIP connection, using a NAT function of the ~~proxy~~ HIP proxy node to route the message to the appropriate destination host.

The above-mentioned query may be a DNS query. The ~~proxy~~ HIP proxy node may intercept the DNS query from the first host. The ~~proxy~~ HIP proxy node may perform the step of retrieving the IP address and HIT associated with the second host.

The ~~proxy~~ HIP proxy node may retrieve the IP address and HIT associated with the second host from an external DNS server. Or the ~~proxy~~ HIP proxy node may retrieve the IP address and HIT associated with the second host from an internal DNS server.

According to a second aspect of the present invention there is provided a communications system comprising a first host which is not HIP enabled, a second host which is HIP enabled, and a ~~HIP proxy~~ HIP proxy node, wherein: the first host comprises means for sending a query to resolve the IP address of the second host; the ~~proxy~~ HIP proxy node comprises means for retrieving, in response to said query, an IP address and HIT associated with the second host, for returning a substitute IP address associated with the second host, for maintaining a mapping between the substitute IP address, the retrieved IP address and the retrieved HIT, and for using the mapping, upon receipt of a session initiation message from the first host including as its destination address the substitute IP address, to negotiate a secure HIP connection between the ~~proxy~~ HIP proxy node and the second host.

According to a third aspect of the present invention there is provided method for use by a ~~HIP proxy~~ HIP proxy node of at least partially securing communications, via the ~~proxy~~ HIP proxy node, between a first host which is not HIP enabled and a second host which is HIP enabled, the method comprising: receiving a query from the first host to resolve the IP address of the second host; in response to said query, retrieving an IP address and HIT associated with the second host, returning a substitute IP address associated with the second host, and maintaining a mapping between the substitute IP address, the retrieved IP address and the retrieved HIT; and upon receipt of a session initiation message from the first host including as its destination address the substitute IP address, using the mapping to negotiate a secure HIP connection between the ~~proxy~~ HIP proxy node and the second host.

According to a fourth aspect of the present invention there is provided a ~~HIP proxy~~ HIP proxy node for use in at least partially securing communications, via the ~~proxy~~ HIP proxy node, between a first host which is not HIP enabled and a second host which is HIP enabled, comprising: means for receiving a query from the first host to resolve the IP address of the second host; means for retrieving, in response to said query, an IP address and HIT associated with the second host, returning a substitute IP address associated with the second host, and maintaining a mapping between the substitute IP address, the retrieved IP address and the retrieved HIT; and means for using the mapping, upon receipt of a session initiation message from the first host including as its destination address the substitute IP address, to negotiate a secure HIP connection between the ~~proxy~~ HIP proxy node and the second host.

According to a fifth aspect of the present invention there is provided an operating program which, when run on a ~~HIP proxy~~ HIP proxy node, causes the proxy to carry out a method according to the third aspect of the present invention.

According to a sixth aspect of the present invention there is provided an operating program which, when loaded into a ~~HIP proxy~~ HIP proxy node, causes the proxy to become one according to the fourth aspect of the present invention.

***Please amend the paragraph beginning at page 14, line 26, as follows:***

FIG. 5, also discussed hereinbefore, is a schematic diagram illustrating the general network set up for communications between a legacy host and a HIP node via a ~~HIP proxy~~ HIP proxy node;

***Please amend the paragraph beginning at page 15, line 9, as follows:***

An embodiment of the present invention will now be described within the general framework of the system described above with reference to FIG. 5. An embodiment of the present invention provides a method of at least partially securing communications between the legacy host 12, which is not HIP enabled, and the HIP host 14, which is HIP enabled via the HP proxy 16 (also referred to as “proxy” (also referred to as “HIP node”) and “HIP proxy node”). Operation of an embodiment of the present invention will now be described with reference to the message exchange diagram of FIG. 6. The steps shown in FIG. 6 are also illustrated in more detail in FIGS. 8 to 12, while FIG. 7 gives a more detailed overview of the packet structures used in TCP, UDP (User Datagram Protocol), ESP and HIP.

***Please amend the paragraph beginning at page 16, line 5, as follows:***

Since the HIP proxy 16 knows that the initiating host that sent the DNS query is not HIP-enabled, the HP proxy 16 does not return the DNS information $\{HIT_{hip}; IP_{fa}\}$. Instead, the HP proxy 16 generates a substitute IP address $IP_{res}$, which in this example is 3ffe:401::5. The HP proxy 16 maintains a mapping $\{HIT_{hip}; IP_{fa}; IP_{res}\}$ between the HIT retrieved from the DNS server 24, the IP address retrieved from the DNS server 24 and the substitute IP address generated by the HP proxy 16. This mapping is required to handle routing of subsequent communications, as will be described below. The generation of the substitute IP address $IP_{res}$ and the maintenance of the mapping is marked as "D" in FIGS. 6 and 9.

***Please amend the paragraph beginning at page 18, line 4, as follows:***

Only one Security Association 22 is set up between the HIP proxy 16 and the HIP node 14, and this Security Association 22 is used by multiple legacy hosts communicating with the same HIP host 14. The above-described mapping M is associated with a Security Association and not with a particular legacy host such as the legacy host 12. Since the Security Association 22, and its associated mapping M, must be used by a plurality of legacy hosts, the mapping M cannot include information relating to a particular legacy host, such as for example the IP address of the legacy host that was initially responsible for setting up the Security Association 22. Instead, the Network

Address Translation (NAT) function in the ~~HIP proxy~~ HIP proxy node handles the mapping of packets to the correct legacy host IP address.